Firepower Threat Defense(FTD)で実行されているアクティブなSnortバージョンの判別

内容

はじめに

このドキュメントでは、Cisco FDM、Cisco FMC、またはCDOによってCisco FTDが管理されている場合に、Cisco FTDが実行するアクティブなSnortバージョンを確認する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Management Center（FMC）
- Cisco Firepower Threat Defense（FTD）
- Cisco Firepower Device Manager（FDM）
- Cisco Defense Orchestrator(CDO)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firepower Threat Defense v6.7.0および7.0.0
- Cisco Firepower Management Center v6.7.0および7.0.0
- Cisco Defense Orchestrator

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

SNORT® Intrusion Prevention System（IPS；侵入防御システム）は正式にSnort 3をリリースしました。これは包括的なアップグレードで、パフォーマンスの強化、処理速度の高速化、ネットワークのスケーラビリティの向上、および200を超えるプラグインの範囲を実現し、ネットワークのカスタムセットアップを作成できます。

Snort 3の利点には次のようなものがあります。

- パフォーマンスの向上
- SMBv2インスペクションの向上
- 新しいスクリプト検出機能
- HTTP/2インスペクション
- カスタムルールグループ
- カスタム侵入ルールを記述しやすくする構文。
- インラインの結果が侵入イベントでドロップされる理由。
- VDB、SSLポリシー、カスタムアプリケーションディテクタ、キャプティブポータルIDソース、およびTLSサーバIDディスカバリに変更が導入されると、Snortは再起動しません。
- サービスアビリティの向上：Snort 3固有のテレメトリデータがCisco Success Networkに送信され、ログのトラブルシューティングが向上します。

Snort 3.0のサポートは、Cisco Firepower Threat Defense(FTD)がCisco Firepower Device Manager(FDM)で管理されている場合に、6.7.0で導入されました。

注:FDMで管理される新しい6.7.0 FTD展開では、Snort 3.0がデフォルトのインスペクションエンジンです。古いリリースから6.7にFTDをアップグレードすると、Snort 2.0がアクティブインスペクションエンジンとして残りますが、Snort 3.0に切り替えることもできます。

注：このリリースのSnort 3.0では、仮想ルータ、時間ベースのアクセス制御ルール、またはTLS 1.1以前の接続の復号化はサポートされていません。Snort 3.0は、これらの機能が不要な場合にのみ有効にしてください。

次に、Firepowerバージョン7.0では、Cisco FDMとCisco Firepower Management Center(FMC)の両方で管理されるFirepower Threat Defense(FTD)デバイスに対するSnort 3.0のサポートが導入されました。

注：新しい7.0 FTD導入では、Snort 3がデフォルトのインスペクションエンジンになっています。アップグレードされた導入は引き続きSnort 2を使用しますが、いつでも切り替えることができます。

注意:Snort 2.0と3.0は自由に切り替えできるので、必要に応じて変更を元に戻すことができます。バージョンを切り替えるたびにトラフィックが中断されます。

注意: Snort 3に切り替える前に、『Firepower Management Center Snort 3コンフィギュレーションガイド』を読んで理解しておくことを強くお勧めします。機能の制限と移行手順に特に注意してください。Snort 3へのアップグレードは影響を最小限に抑えるように設計されていますが、機能が正確にマッピングされるわけではありません。アップグレード前の計画と準備は、トラフィックが期待どおりに処理されることを確認するのに役立ちます。

FTDで稼働しているアクティブなSnortバージョンの確認

FTDコマンドラインインターフェイス(CLI)

FTDで実行されているアクティブなSnortのバージョンを確認するには、FTD CLIにログインして、show snort3 statusコマンドを実行します。

例1：出力が表示されない場合、FTDはSnort 2を実行します。

```
<#root>

>

show snort3 status

>
```

例2：出力に「Currently running Snort 2」と表示されている場合、FTDはSnort 2を実行しています。

```
<#root>

>

show snort3 status

Currently running Snort 2
```

例3：出力に「Currently running Snort 3」と表示されている場合、FTDはSnort 3を実行しています。

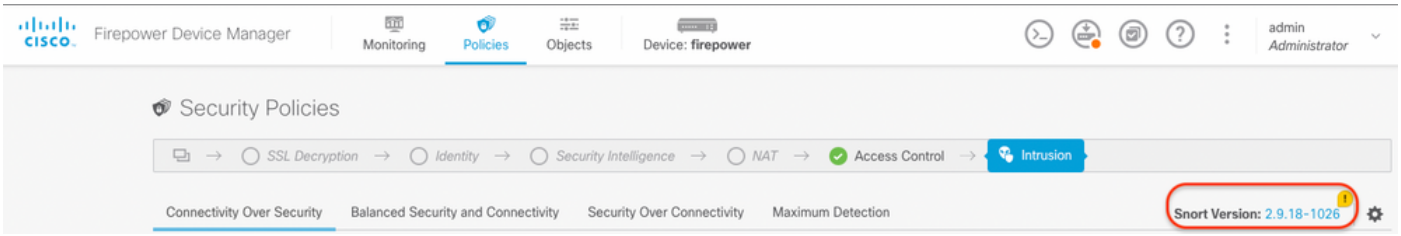
```
<#root>

>

show snort3 status


Currently running Snort 3
```

Cisco FDMによるFTDの管理

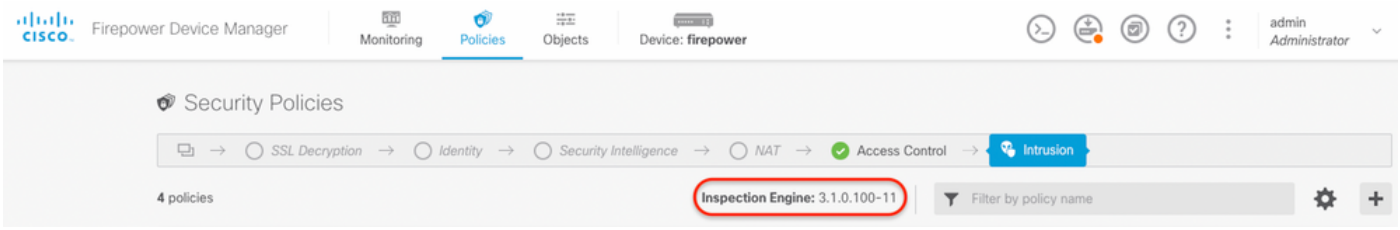
Cisco FDMによって管理されているFTDで実行されているアクティブなSnortのバージョンを確認するには、次の手順を実行します。

1. FDM Webインターフェイスから Cisco FTDにログインします。
2. メインメニューからPoliciesを選択します。
3. 次にIntrusionタブを選択します。
4. Snortのバージョンまたは「インスペクションエンジン」セクションを探して、FTDでアクティブなSnortのバージョンを確認します。

例1:FTDがSnortバージョン2を実行している。



例2:FTDがSnortバージョン3を実行している。

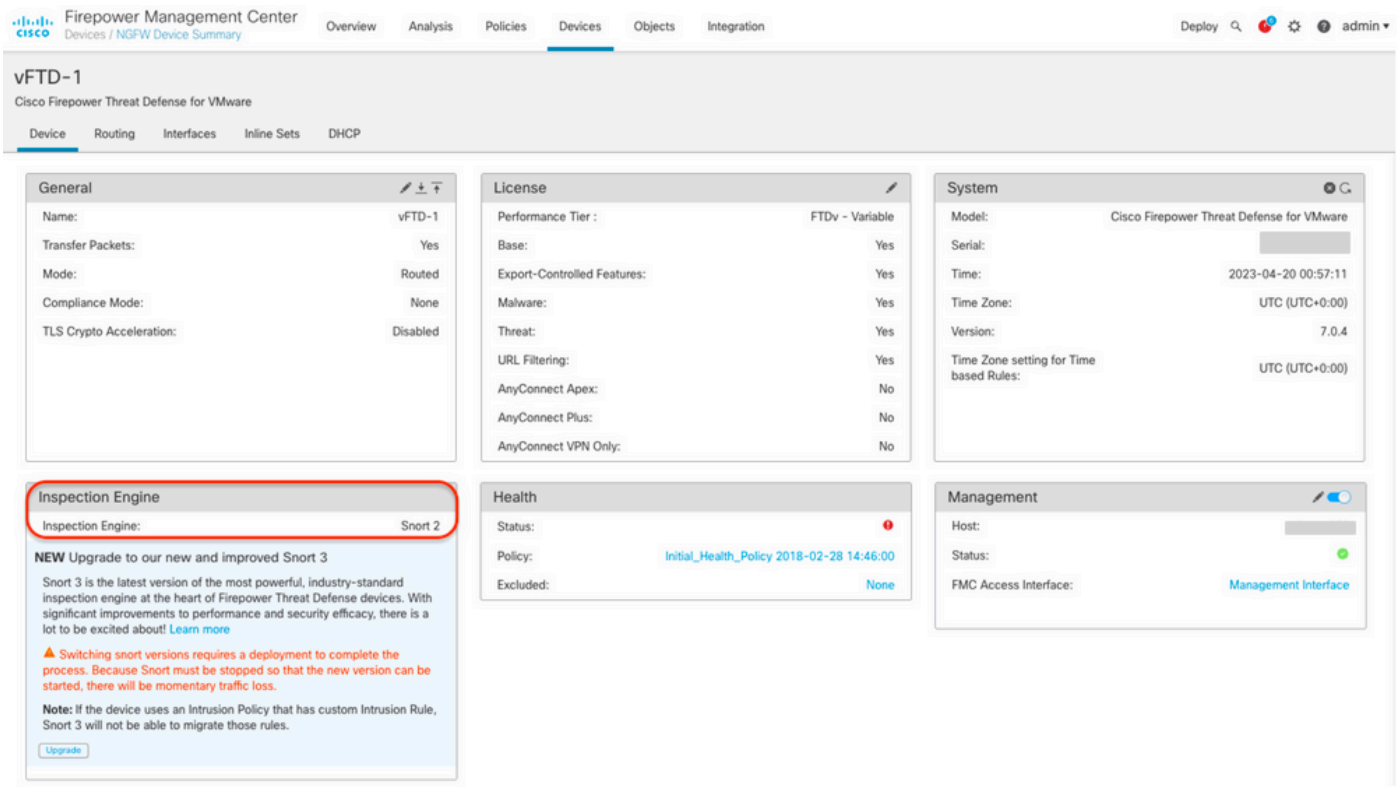


Cisco FMCによって管理されるFTD

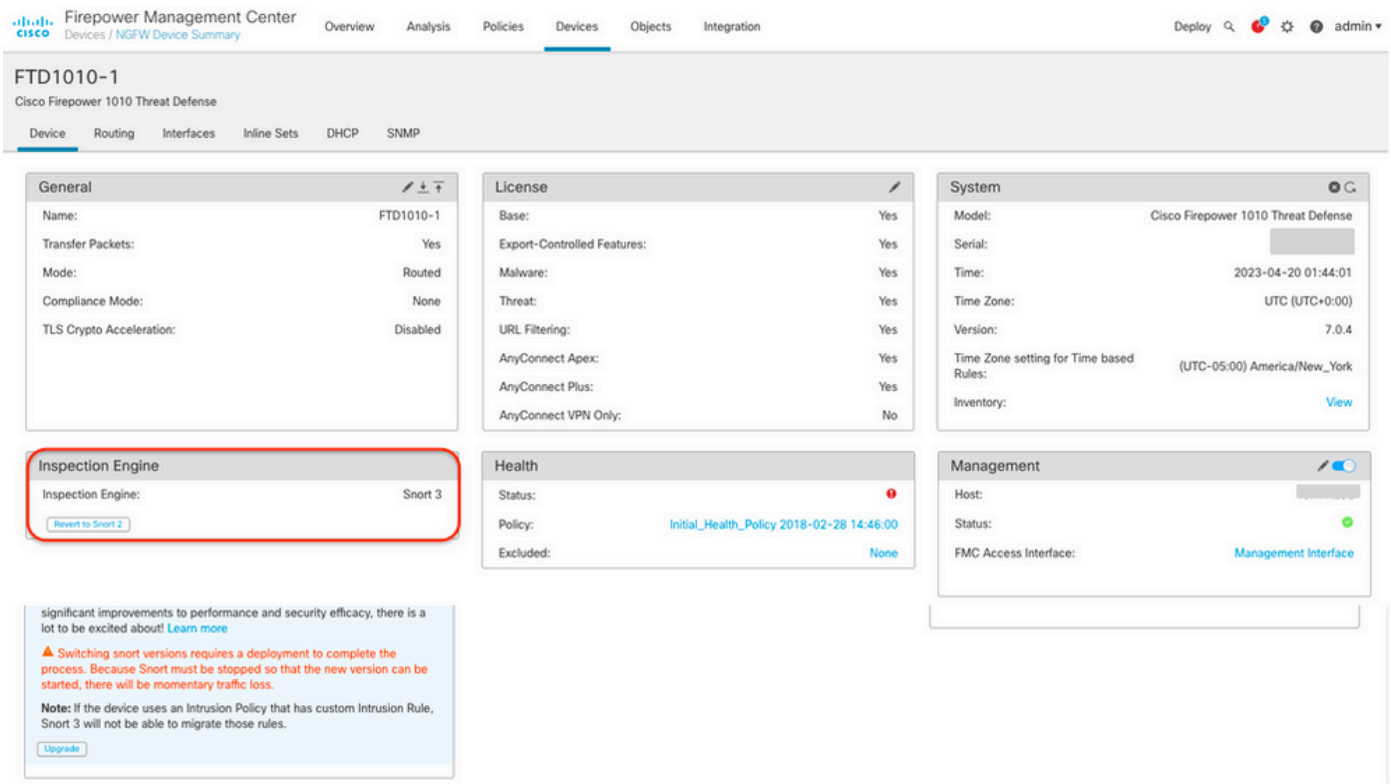
Cisco FMCによって管理されているFTDで実行されているアクティブなSnortのバージョンを確認するには、次の手順に従います。

1. Cisco FMC Webインターフェイスにログインします。
2. DevicesメニューからDevice Managementを選択します。
3. 次に、適切なFTDデバイスを選択します。
4. [編集（Edit）] アイコン（鉛筆の形）をクリックします。
5. Deviceタブを選択し、Inspection Engineセクションを探して、FTDでアクティブなSnortのバージョンを確認します。

例1:FTDがSnortバージョン2を実行している。



例2:FTDがSnortバージョン3を実行している。



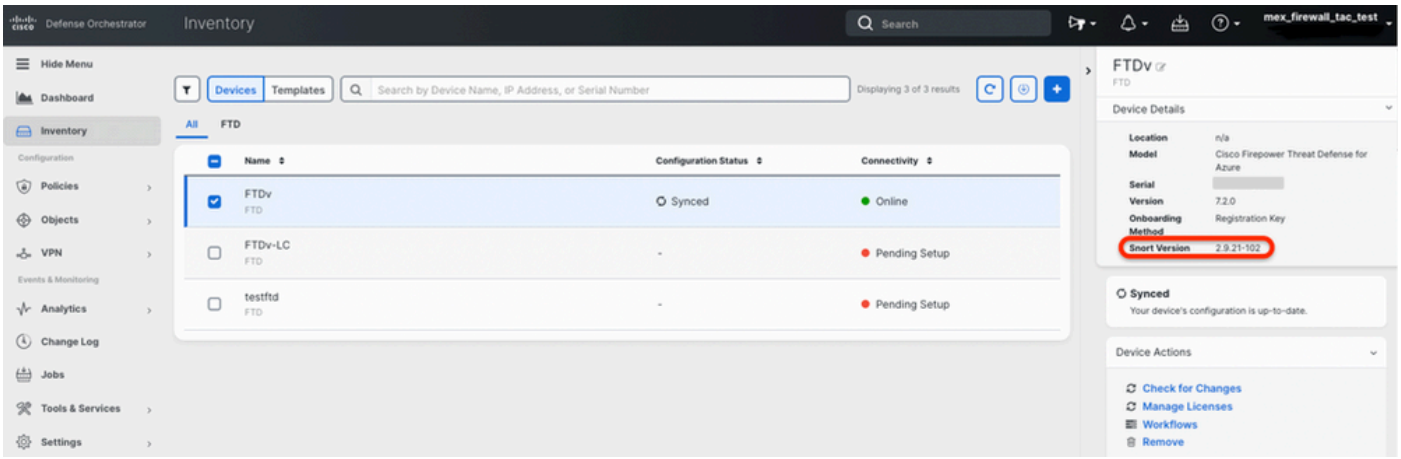
Cisco CDOによって管理されるFTD

Cisco Defense Orchestratorによって管理されているFTDで実行されているアクティブなSnortの

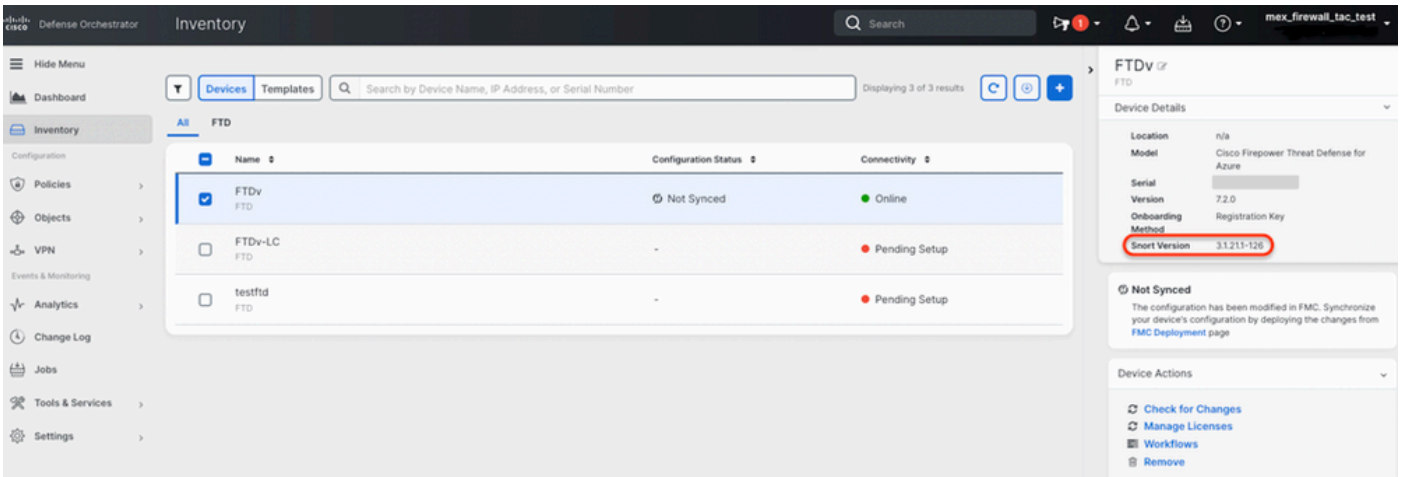
バージョンを確認するには、次の手順に進みます。

1. Cisco Defense Orchestrator Web インターフェイスにログインします。
2. Inventoryメニューから、適切なFTDデバイスを選択します。
3. Device Detailsセクションで、Snort Versionを探します。

例1:FTDがSnortバージョン2を実行している。



例2:FTDがSnortバージョン3を実行している。



関連情報

- Cisco Firepowerリリースノート、バージョン6.7.0
- Cisco Firepowerリリースノート、バージョン7.0
- Snort 3のWebサイト
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。